Australian Government
Department of Defence
Defence Science and
Technology Organisation

DSTO

Technical Risk Assessment of Australian Defence Projects

Jim Smith, Graeme Egglestone, Paul Farr, Terry Moon, David Saunders, Peter Shoubridge, Kym Thalassoudis and Tony Wallace

DSTO-TR-1656

Australian Government
Department of Defence
Defence Science and
Technology Organisation

Technical Risk Assessment of Australian Defence Projects

DSTO Tiger Team for Technical Risk Assessment:

Jim Smith (Chairman), Graeme Egglestone, Paul Farr, Terry Moon
David Saunders, Peter Shoubridge, Kym Thalassoudis and Tony Wallace

Defence Systems Analysis Division
Information Sciences Laboratory

DSTO-TR-1656

ABSTRACT

The Defence Procurement Review (DPR) recommended sweeping changes to Defence Department structures, policies, processes and procedures for the acquisition of military capabilities. As a result of the Government's acceptance of the recommendations of the DPR, DSTO roles and responsibilities now include guidance on, and certification of, Technical Risk Assessments (TRA) for major acquisition proposals up to second-pass approval. This paper provides a structured approach for the undertaking of TRA and their subsequent certification. Also included are discussions of the underpinning principles, techniques and tools, training requirements and resource implications.

RELEASE LIMITATION

Approved for public release

Published by

DSTO Information Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-013-285
December 2004

APPROVED FOR PUBLIC RELEASE

Technical Risk Assessment of Australian Defence Projects

Executive Summary

The Defence Procurement Review by Malcom Kinnaird in 2003 suggested sweeping changes to Defence Department structures, policies, processes and procedures for the acquisition of military capabilities. As a result of the government's acceptance of the review's recommendations, DSTO has been recognised as having a responsibility for the review and sign-off of technical risk assessments (TRA) up to second-pass approval. In addition to this certification of TRA, DSTO may be called upon to assist in the undertaking of TRA for specific projects.

To ensure that assessments of technical risk are coherent, consistent, comprehensive and credible, a structured approach to assessing technology readiness and technical risk has been developed. This new approach has been tailored for the Australian Defence Organisation (ADO) but is based on four fundamental principles, namely, that the approach:

1. Is consistent with the Australian Defence capability development cycle, i.e. it should fit naturally with the zero (entry into the Defence Capability Plan), first and second-pass decision points and be focused to provide the information required at these key decision points.
2. Is based on the universally recognised scheme of Technology Readiness Levels (TRL) as recommended by Kinnaird.
3. Is based on the principles for risk management given in the Australian Standard (AS/NZS 4360:2004). This emphasises that risk assessment links consequences and likelihood and identifies the role of expert judgement.
4. Takes account of systems issues such as integration and implementation.

Figure E.1 outlines the TRA process up until second-pass approval. As proposals progress through key decision points, it is envisaged that the focus would shift from technology readiness (i.e. the maturity and feasibility of technologies) to the technical risk associated with systems, their integration with other systems and their implementation in Australian military operations. This would reflect a higher degree of understanding of the technical issues as more information becomes available. Technology maturity and feasibility would be assessed using Technology Readiness Levels (TRL) as recommended by the Defence Procurement Review while systems integration and implementation issues would be addressed through Systems Readiness Levels (SRL). Questions that frame assessment at each decision point have also been developed.

Certification of technology readiness and technical risk, along with specific support to Projects for technical risk assessment and risk mitigation, will result in significant additional work for DSTO. Specific training will be required to ensure a consistent approach and timely responses.

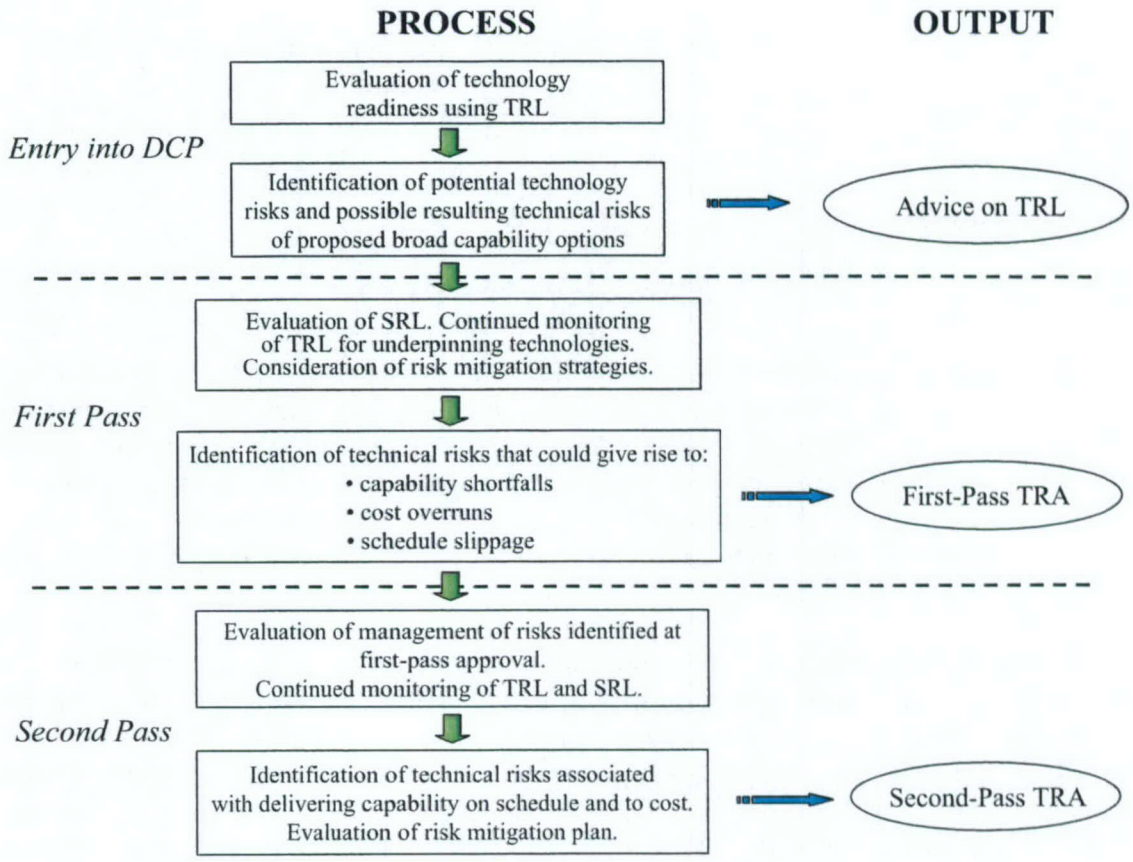


Figure E1: Proposed technical risk assessment process.

General questions to be asked at all decision points are:

1. What are the technical issues and drivers? (For new technologies, this might include discussion of the lack of historical information on life-of-type, durability, maintainability, etc.)

2. What maturity currently exists, both in the underpinning technologies and the integrated system (i.e. current TRL and SRL)?

3. What needs to be done to refine the development?

4. What resources are required and how long will it take?

Authors

Tiger Team for Technical Risk Assessment
Defence Science and Technology Organisation

The Defence Procurement Review (DPR) suggested sweeping changes to Defence Department structures, policies, processes and procedures for the acquisition of military capabilities. Directly affecting DSTO is the recommendation of 'a strengthened capability definition and assessment function' and the proposal to introduce a 'strengthened two-pass system' for capability development.

As a result DSTO formed a DPR Consultation and Implementation Team (DCIT) comprising four Tiger Teams: Policy, Code of Best Practice (COBP), Forward Analysis Planning (FAP) and Technical Risk Assessment (TRA). The TRA Tiger Team was directed to develop a suitable approach to TRA within the context of the DPR, the new roles and responsibilities for DSTO arising from it and current best practice.

The pan-DSTO team initially comprised Jim Smith (PSL Executive HQ), Graeme Egglestone (CBRN), Terry Moon (DSAD) and Peter Shoubridge (IND). The team was subsequently expanded to include David Saunders (MPD), Kym Thalassoudis (WSD), Tony Wallace (SA-DMO) and Paul Farr (MOD).

Contents

LIST OF ABBREVIATIONS

DEFINITIONS

1. INTRODUCTION 1
   - 1.1 DSTO Roles and Responsibilities 1
   - 1.2 Project Types 1

2. RISK DEFINITIONS 3
   - 2.1 'Technology' Readiness and 'Technical' Risk 4
     - 2.1.1 Technology Readiness 4
     - 2.1.2 Technical Risk 4
   - 2.2 Context 4

3. TECHNIQUES AND TOOLS 5
   - 3.1 Technology Readiness Levels 5
   - 3.2 Addressing Systems Issues 6
   - 3.3 System Readiness Levels 6

4. TECHNICAL RISK ASSESSMENT 7
   - 4.1 Principles 7
   - 4.2 Process 7
     - 4.2.1 Entry into the DCP 8
     - 4.2.2 First-pass Approval 9
     - 4.2.3 Second-pass Approval 9
   - 4.3 Risk Assessment 10

5. CERTIFICATION 11
   - 5.1 Pro forma 11

6. TRAINING 11
   - 6.1 Courses for selected staff 11
   - 6.2 Pathways 12
   - 6.3 Continuing Education Initiative (CEI) 12
   - 6.4 GPSL and RESMAN 12
   - 6.5 Elements of TRA Training Courses 12
   - 6.6 Priorities for Training 13

7. RESOURCES 14

8. CONCLUSIONS 15

9. ACKNOWLEDGEMENTS 15

10. REFERENCES 15

APPENDIX A: TECHNOLOGY READINESS LEVELS 17

APPENDIX B: SYSTEM READINESS LEVELS (SRL) 20
B.1. Short version 20
B.2. Longer version 20

APPENDIX C: TRL, SRL AND TRA RELATIONSHIP 22

APPENDIX D: GUIDELINES FOR ASSESSING TECHNICAL RISK 23

APPENDIX E: TRA COURSE OUTLINE 24

List of Abbreviations

ADF	Australian Defence Force
ADO	Australian Defence Organisation
CDG	Capability Development Group
CDP	Capability Development Process
CEI	Continuing Education Initiative
DCP	Defence Capability Plan
DMO	Defence Materiel Organisation
DPR	Defence Procurement Review
DSTO	Defence Science and Technology Organisation
FAP	Forward Analysis Plan
HW	Hardware
IPT	Integrated Project Team
KIP	Key Integration Parameters
NASA	National Aeronautics and Space Administration
OTS	Off-The-shelf
PBT	Practice-based Technologies
S&T	Science and Technology
SW	Software
SRL	System Readiness Levels
TRA	Technical Risk Assessment
TRL	Technology Readiness Level
US DoD	United States Department of Defense
UK MoD	United Kingdom Ministry of Defence

Definitions

Technology risk
The risk that an underpinning technology, necessary for a capability, will not mature within the required timeframe.

Technical risk
The risk that a system will not reach its performance goals, development will not be within the specified timeframe and/or it will cost more than estimated due to technical development and maturity risks.

1. Introduction

1.1 DSTO Roles and Responsibilities

The Defence Procurement Review (Kinnaird 2003) (DPR) recommended the use of 'standardised Technology Readiness Levels' (TRL) and noted that 'DSTO would be capable of using this methodology to rate technical risks for new capabilities'. Acceptance of the recommendations of the Defence Procurement Review by Government means that DSTO now has a primary role to advise on technology and technical risk issues relating to Defence's capability options under the Defence Capability Plan (DCP) and acquired through the Capability Development Process (CDP). DSTO also has the responsibility to provide certification of Project Technical Risk Assessments (TRA) at 1st and 2nd pass approval stages of the CDP. The results of the review of Project TRA are represented in the CDP by the Chief Defence Scientist (CDS) who carries responsibility for certification of the TRA.

In response to the recommendations of the Defence Procurement Review, DSTO is developing policy, processes and procedures to undertake its role in providing advice on technical risk issues and for certification of TRA undertaken by major Projects. Risk management in the CDP continues after second-pass but becomes the responsibility of the Defence Materiel Organisation (DMO).

1.2 Project Types

Australian Industry is not a major developer of new military capabilities and so the defence capabilities of the Australian Defence Force (ADF) are usually sourced from overseas companies. Australian Industry may have the role of component or sub-systems supplier, or as a partner with overseas companies for the supply of capital assets including ships, aircraft and land vehicles and other defence systems and equipment. It cannot be assumed that Industry will be able to address all the technical risks associated with the introduction of new capabilities into the Australian Defence Force (ADF). Hence, technical risks faced by the Australian Defence Organisation (ADO) should be assessed as part of the CDP.

Following the acceptance of the recommendations of the DPR, it is now mandated within the CDP that, when acquiring new capability, the ADO must consider at least three options: one: off-the-shelf (OTS) option (usually sourced from overseas), two: a modified OTS option and three: another that meets all capability requirements. The OTS option provides a baseline against which the ADO would assess other capability options. Along with assessment of the capabilities proposed to address the Defence requirement, the assessment also involves consideration of technical, cost and schedule risks.

Although the OTS option will represent a current capability, this option can still, however, involve technical risk from an Australian perspective. Most importantly, however, all capability options potentially have risks associated with them. These may include technical, cost, schedule and capability risks. DSTO is primarily concerned with understanding technology and technical risks and ensuring that Project TRA are comprehensive and consistent, and that they properly address technical issues that

could impact on the capability, cost or schedule for the acquisition of new defence capabilities.

Technical risk assessment may present some significant problems; for example, the ADO may have limited access to sufficiently detailed technical information with which to undertake risk assessment. Additionally, technology maturity assessments, and the results of operational test and evaluation from overseas suppliers and operators may not be applicable to the Australian environment (or for the Australian Defence Force's intended use). Integration risks may also be difficult to assess in the absence of comprehensive technical information.

The DPR mandated the use of Technical Readiness Levels (TRL) to indicate the maturity of the critical technologies underpinning the capability delivered by proposed options. TRL are measured on a scale of 1 to 9, starting with paper studies of the basic concept, proceeding through laboratory demonstrations, and ending with a technology that has proven itself in operational service.[1] TRL are reassessed throughout the progress of the Project to monitor the maturation of the technologies and to determine consequences for technical risk.

Table 1 categorises projects,[2] and provides a broad indication of the degree of development needed to achieve project outcomes and the likely science and technology (S&T) involvement required. The table also provides an indication of the likely TRL at the commencement of the capability development process.

The general principles under which the ADO will conduct its TRA process are set out AS/NZS 4360:2004 (Standards Australia 2004) which is also consistent with the US DoD approach (US DoD 2004b).

[1] See US DoD 2004a, Graettinger *et al.* 2002 or Kinnaird 2003 for descriptions of TRL.
[2] This categorisation applies between first and second-pass approval.

Table 1: Project Types.[3]

Project Type	Off-the-shelf	Integration	Integration with modification	Bespoke
Focus	Best available of OTS options.	Improvement	Optimising to meet specific requirements. OTS options not available.	New, custom-made for purpose.
Example	F/A-18	F/A-18 HUG	Wedgetail, Collins	JORN, Nulka
Issues	Understanding purpose and design	Integrating OTS components for a specific purpose.	Integrating off the shelf components with significant modifications.	Design ownership. More uncertainty of outcomes. Significant resources required to progress to TRL 9.
Development Needed	Minimal	Limited	Significant	End-to-end
S&T involvement required	Minimal	Limited	Substantial	Major
Typical TRL at start of process	8-9	6-8	5	3-4

2. Risk Definitions

AS/NZS 4360:2004 provides the key definitions used in risk management. The standard defines 'risk' as '*the chance of something happening that will have an impact upon **objectives***'.[4] Objectives from a risk and risk management sense need to be clearly identified. This risk management standard also states that risk '*is measured in terms of **consequences** and **likelihood***'. AS/NZS 4360:2004 gives some examples of generic sources of risk including '*technology and technical issues both internal and external to the organisation*. Additionally, a lack of detailed technical information, uncertainty about future developments and insufficient domain knowledge and experience can also contribute to risk.

Consequences are defined by AS/NZS 4360:2004 as '*the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event*'. **Likelihood** is defined as '*a qualitative description of probability or frequency*'.

[3] The Capability Systems Lifecycle Manual lists project types as (i) modifying existing platforms, (ii) acquiring OTS options (Commercial and Military), (iii) acquiring and modifying OTS, (iv) integrating existing systems, (v) pursuing new designs. The table above does not differentiate between (i) and (iii).

[4] Risk is assessed for a defined event or circumstance and is measured as a combination of the consequences that may flow from that event and their likelihood. Risk may have a negative or positive impact.

2.1 'Technology' Readiness and 'Technical' Risk

2.1.1 Technology Readiness

Technology readiness may be thought of as 'the status of an underpinning technology with respect to its feasibility and maturity for operational use'. TRL were suggested by Kinnaird (2003) and are being widely used elsewhere (US DoD 2004a; Graettinger *et al.* 2002; UK MoD 2002). In this context, TRL provide a widely used and accepted means to assess technology maturity at each decision point in the capability development lifecycle. In the initial stages, TRL would be used as a simple filter for assessing technology readiness (i.e., maturity and feasibility) of new technologies or novel use of existing technologies. TRL would thus give an indication of the technical challenge ahead. At later stages of the CDP, the emphasis would shift to monitoring whether technologies are transitioning as expected.

2.1.2 Technical Risk

Technical risk may be defined as 'the risk that a system will not reach its performance goals, development will not be within the specified timeframe and/or it will cost more than estimated due to technical developmental and maturity risks' (Moon, T., Smith, J., Nicholson, J, Fewell, S. & Duus, A. 2004). While technical risk would be assessed at all decision points in the CDP, the focus of the technical assessment would change at each successive decision point as the number of options under consideration is reduced and more technical information becomes available. Major technical risks for projects include problems, difficulties and unexpected outcomes arising from:

1. Defining, interpreting and managing operational requirements.
2. Systems configuration and integration.
3. Interoperability. This includes interfaces with both existing and proposed systems (including contingency alternatives) and interoperability within the wider ADF and in operations with allies.
4. Test and Evaluation.
5. Operating and support aspects (including maintenance, personnel skills and training, information access and management).
6. Further development and through-life upgrades.

2.2 Context

Technology Risk Assessments concentrate on the underpinning technologies critical to the system capability, and are generally assessed at the sub-system level. Technical risk assessments consider risks to the delivery of the required capability by the integrated system. It is important that the technical risk of capability options are assessed within the context of the required Defence capabilities. While an underlying technology risk could be assessed as low, the technical risk could still be high because of integration issues, environmental issues, interoperability and possible dependence on other (as yet untested) technologies.

3. Techniques and Tools

3.1 Technology Readiness Levels

Many US DoD programs now use technology readiness levels (TRL) to assess the maturity level of technology and to identify the risk that technology poses if it were to be included in a product development. Similarly, TRL are being used in the UK (UK MoD 2002). Brock (2004) notes that the higher the TRL, the smaller the gap between the technology's maturity and the product's requirements, and the lower the risk of including the technology in the product's development. 'Best practices work' has shown that a TRL=7 (demonstration of a technology in an operational environment) is the minimum level of readiness required to achieve acceptable risk when committing to an acquisition programme.

It should, however, be noted that Brock is considering capability development from a US perspective where new capabilities are developed from their inception at TRL 1 through to a mature product at TRL 9. The demonstration for TRL 7 would thus be in an operational environment of specific relevance to the US. For Australia, the US threshold of TRL 7 may not fully address Australia's requirements, and there may not be sufficient technical and operational details available to make a definitive judgement of technology readiness for Australian military operations. Use of the US-evaluated minimum threshold of TRL 7 is thus not recommended, without critical consideration of the relevance of demonstration activities supporting their contribution to assessment of Australia's capability needs.

TRL 7 is a key milestone in technology development because it means that the technology has been matured to the point where prototype demonstration has occurred in the relevant operational environment. The significance of TRL 7 should not, however, preclude early investment in R&D programs necessary to mature and demonstrate high-risk, high-performance TRL 4 to 6 technologies to a level acceptable for inclusion in product acquisition programs.

In reviewing current literature on TRL, Graettinger *et al.* (2002) point out that most references are limited to the context of using TRL to improve the timing of transitioning or inserting a technology from the demonstration phase to product development. Indeed, US DoD acquisition regulations emphasize the need to separate technology development from product development. Experience shows that trying to resolve technology problems during product development can result in very significant cost increase and schedule slippage. US DoD regulations require that military project managers 'conduct a technology readiness level assessment for critical technologies identified in major weapon systems programs prior to the start of engineering and manufacturing development and production'.

Similarly the UK Ministry of Defence (MoD) (2004) regard the TRL framework as 'designed to be used in relation to individual technologies and therefore below the level of the complete system'. Thus TRL are not designed to explicitly take account of systems configuration, integration and implementation aspects. It is for this reason that a distinction is drawn between Technology Risk Assessment and Technical Risk Assessment.

NASA originally developed TRL definitions for hardware technologies only. Additional descriptions have since been developed separately for software (Graettinger *et al.* 2002), and for practice-based technologies, i.e. practices, processes, methods, approaches and frameworks (Graettinger *et al.* 2003). These definitions can be brought together in one table to provide a broad schema for evaluating technology readiness (see Appendix A). Definitions for hardware and software have been brought together in the 'TRL Calculator' - a software tool developed by William Nolte of the US Air Force Research Laboratory (Defense Acquisition University 2004). This tool comprises structured questions to facilitate evaluation of a TRL for a particular technology.

Assessment of TRL before entry to the DCP may be undertaken by DSTO, and is based on knowledge gained through DSTO's role of monitoring technology developments of potential significance for Defence ('technology watch') and its participation in National and International research arrangements. TRL will be reassessed throughout the progress of the Project to monitor the maturation of the technologies and to determine the consequences for technical risk arising from any changes made.

3.2 Addressing Systems Issues

As already indicated TRL do not provide a technical risk assessment for a total system. While they can be applied in a hierarchical manner, careful consideration of integration risks for the total system will be necessary irrespective of the level of application of TRL (UK MoD 2004).

A project might, for example, have a collection of sub-system technologies that have reached TRL 9, but at the system level the sub-systems have not been well integrated, and thus the total system has a low level of 'readiness' with significant residual technical risk. As an example, consider the design of a multi-sensor, surveillance and reconnaissance aerial system. The platform could be a readily available aircraft that is tried and tested, but integrating a suite of sensors, even if commercially available, involves addressing integration issues ranging from weight and centre of gravity effects on the airframe through location of sensor heads so as to provide a clear fields of regard, to the potential for electromagnetic interference and how best to process, combine and display the information provided by the sensors. This is a demanding process, and it can readily be appreciated that TRL at the sub-system level are not able to provide a complete picture of system technical risk.

3.3 System Readiness Levels

The UK MoD (2004) has introduced System Readiness Levels (SRL) to assess system maturity and thus support project planning. The nine levels chosen in the SRL scale reflect those used in the TRL schema but have been aligned to accepted systems engineering stages. Progression from lower to higher numbers indicates increasing system maturity (readiness for operational use). The iterative nature of the systems development process, and the potential for concurrent design activities in the sub-systems, is specifically noted. In addition the SRL schema contains Key Integration Parameters (KIP) to guide analysis and inform judgement on overall system readiness. KIP also provide a means of monitoring and managing technical risk. The UK MoD schema is detailed but the principles it is based on can be understood from the descriptions given in Appendix B.

In the progression of a Project through the CDP the focus shifts from the risks associated with underlying technologies of proposed options to the issues of systems configuration, integration and implementation. As SRL readily address these systems issues, and augment the TRL scale, it is recommended that they be used as the primary measure for TRA in second-pass approval.

4. Technical Risk Assessment

4.1 Principles

The process and procedures recommended for assessing technology readiness and technical risk are based on the following fundamental principles:

1. The risk assessment process should be integral with the capability development life cycle process, i.e. it is tailored to providing the required information at the relevant decision points i.e. entry into the Defence Capability Plan (DCP), first-pass and second-pass approval
2. The use of TRL as recommended by Kinnaird (2003).
3. Conformity with the principles for risk management given in the Australian Standard (AS/NZS 4360:2004). This standard emphasises that risk assessment links consequences and likelihood and identifies the role of expert judgement.
4. Consideration of system issues such as integration and implementation.
5. Consideration of risk mitigation strategies.

Technical Risk Assessment and the assessment of Technology Readiness Levels are judgement-based and the outcomes are dependent on the domain knowledge and experience of the subject matter experts involved. It is important to note that the requirement to address integration issues may involve additional skills that technology domain experts may not necessarily possess.

4.2 Process

The three decision points relevant to TRA in the capability development life cycle are:

1. Entry into the Defence Capability Plan (DCP)
2. First-pass approval: assessing broad capability options.
3. Second-pass approval: assessing and costing the realistic options approved at first-pass.

As Projects progress through these decision points, it is envisaged that the focus would shift from technology readiness (i.e. the maturity and feasibility of technologies) to the technical risk associated with systems, their integration with other systems, and their support and operation to meet Australian military applications.

Prime questions (PQ) to be answered at all decision points are:

1. Is the proposal technically sound? [PQ1]
2. Is it likely to work as required by the prime Customer [PQ2]
3. Will the proposal meet Australian capability requirements? [PQ3]

4. To what degree, and how, will the risks in this proposal adversely affect, or be affected by, other projects planned or currently in progress across the ADF? [PQ4]

If the option assessed is being developed specifically for Australia as prime Customer, then Q3 subsumes Q2.

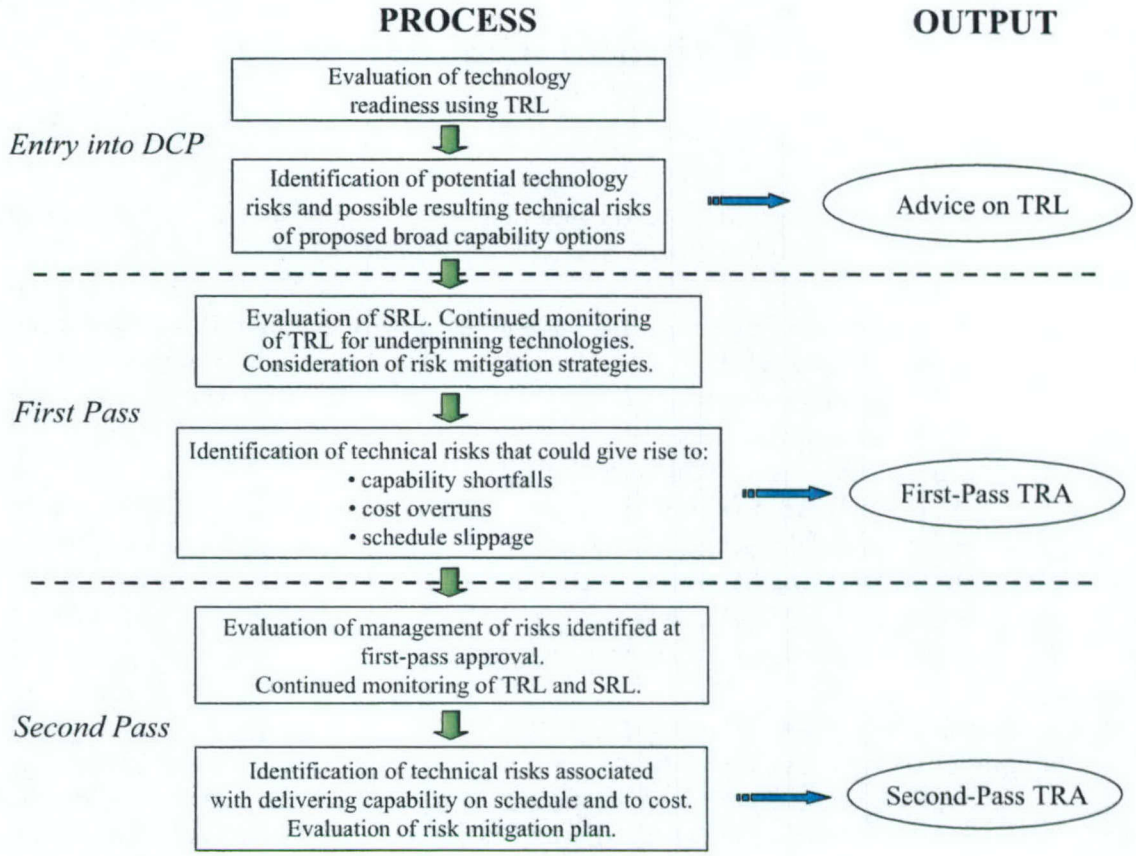


Figure 1: Technical risk assessment process.

Figure 1 illustrates the process for TRA up to and including second-pass approval. The results of the evaluation of technology readiness using TRL, in addition to an assessment of the technical risks for the overall system, provide the basis for Defence Technical Risk Assessment. For many technologies, the expertise required for the assessment of technology readiness is available from within DSTO. This may, however, be supplemented by specialist advice from academia or appropriate contractors when necessary.

4.2.1 Entry into the DCP

General questions for this decision point are:

1. What are the technical issues and drivers? (For new technologies, this might include discussion of the lack of historical information on life-of-type, durability, maintainability, etc.)
2. What maturity currently exists (i.e. current TRL)? At this stage TRL may be used to filter the potential approaches to capability development.
3. What needs to be done to refine the development?

4. What resources are required and how long will it take?

At this stage, the focus is on a TRL assessment where the maturity and feasibility of the broad underpinning technologies are evaluated. This might include the estimation of the timeframes and likely resources needed to bring the technology to fruition. Any assumptions should also be stated. Prior to entry into the DCP, the ability of the Defence Industry base to develop and/or deliver the capability should also be examined.

4.2.2 First-pass Approval

The same 4 general questions asked prior to entry into the DCP also apply at first-pass. The focus is, however, on capability shortfalls and potential adverse consequences, *i.e.* on cost and schedule (but still in general terms). With the broad capability options reduced, assessment is focused on the functional components of the system, *e.g.* platform, mission system and system issues (including integration, interoperability and the ability of the system to meet requirements). TRL are reassessed to monitor the maturation of technologies and to determine consequences for technical risk.[5] The risk assessment reflects a higher degree of understanding, as more technical information becomes available.

Some specific questions for first-pass are:

1. Will the program be sustained and run to completion? Issues that could be addressed for an overseas development program include the credibility of the program in terms of political and military support, the ability of the supplier to meet the primary customer's requirements and whether there is an available substitute. Where a technology is mature it is also important to consider if the production run is likely to be sustained during the anticipated life of the capability in the ADF.
2. Will the program succeed technically? In this context, success is measured in terms of meeting the primary customer's requirement. This depends on the maturity of the technologies employed in the various systems, the criticality of individual systems to the success of the program, the likely success of integration and the extent to which requirements exceed state-of-the-art.
3. Will it work as a system?
4. Will the system meet Australian requirements?
5. Will technical risk affect the affordability of the system?
6. Will the system integrate successfully with the rest of the ADF and interoperate with allies?

4.2.3 Second-pass Approval

The general and specific questions asked at first-pass again frame assessment for second-pass approval but at second-pass the favoured options are assessed in more detail. In particular there should be a focus on ensuring that any risk mitigation activity identified at first-pass is generating the expected outcomes, and at ensuring that greater knowledge of the options obtained during the assessment phase has not revealed additional risks. This includes consideration of technical and other dependencies arising from the proposed operational concepts and from integration with other Projects and ADF assets. Technical risk assessment at this stage examines identified technical risks in

[5] This needs to include potential enhancements to capability so that they are not overlooked.

detail. Assessment should also include evaluation of the ability of prospective Contractors to deliver the capability sought.

At second pass, the proposed contractual mechanism will have been identified, and more detailed attention should be given to the probable impacts of the identified risks. Where an assessment is provided on 3rd party and Project-generated risk assessments, attention should be paid to ensuring the completeness of the risk assessment; to validating the likelihood and impact assessments; and to advising on the credibility and likely effectiveness of proposed risk management measures.

4.3 Risk Assessment

To facilitate the risk assessment it is convenient to categorise the likelihood and the severity of adverse consequences (i.e. impact). For likelihood, the following schema applies (AS/NZS 4360:2004):

LIKELY	POSSIBLE	UNLIKELY
More likely to happen than not (i.e. a probability of greater than 50%).	Everything judged as being between LIKELY and UNLIKELY.	Less than one chance in five of happening.

This approach has been taken because a likelihood of greater than 50% indicates that the risk event is more likely to happen than not, and as such, should therefore be considered to be part of the project context. Given this, those risks that will have adverse consequences for the program will require management and mitigation if the program is to succeed.

To assess the impact, i.e. severity of adverse consequences:
"**Major**" indicates that, should the adverse consequences eventuate, and remediation is not possible, the program may no longer be achievable. [6]
"**Moderate**" indicates definite and significant adverse consequences, but not in themselves sufficient to invalidate the program.
"**Minor**" indicates that, although there would be some adverse consequences that could not be addressed, they would not be expected to have a major effect on the utility or affordability of the system.

Risk assessment would then be in a form shown by Table 2. [7]

Table 2: Risk Assessment.

	Consequence/Impact		
Likelihood	Minor	Moderate	Major
Likely			
Possible			
Unlikely			

Overall TRA indicator: Red (high); Amber (medium); Green (low).

[6] Of concern for major capital acquisition projects are cost overruns, schedule slippage and capability shortfalls.
[7] This is congruent with the US DoD approach to risk assessment (US DoD 2004b).

N.B. It is suggested that where a potential risk has been identified but judged to be inconsequential it should be explicitly stated as such.

Specific account should be taken of all the risks with major impact (right-hand column), and those that are considered likely (top row) with particular emphasis on those that fall in the top right-hand corner.

In most cases, risks will have adverse consequences. However, events with beneficial and high-payoff consequences should also be noted so that significant enhancements to capability are not overlooked.

Systems Readiness Levels (SRL), as given in Appendix B, augment the use of TRL. These provide a means of evaluating the readiness of a system to provide the military capability sought. In the early stages of the CDP the focus will be on the feasibility of the underlying technologies, their maturation and the risks associated with bringing them to the point of an operational capability. As a Project progresses through the CDP the focus will shift to systems configuration, integration and implementation issues.

5. Certification

Routinely, the project DSTO POC is responsible for completion of the review of the TRA, drawing on 'whole of DSTO' resource as required. The TRA has to be approved by the relevant COD and presented by CDS.

5.1 Pro forma

Pro forma have been developed for certification of TRA use at first and second-pass approval. These are based on the principles espoused in this document and call for evaluations of TRL and SRL with supporting information. They are available on the DSTO Intranet.

6. Training

Technical risk assessment is an important element of the Capability Development Process, and the recent Defence Procurement Review has resulted in a mandated role for DSTO in the certification of Project TRA. It is thus important that DSTO develops and maintains expertise in conducting TRA, and in certifying third-party TRA for the full range of Defence capability investment. This will require training to ensure that risk assessment and risk management skills become part of DSTO culture, a consistent approach is taken across DSTO and that best practices are followed.

6.1 Courses for selected staff

At this early stage in the introduction of TRA to DSTO, there is a clear need for key staff, including all project S&T advisers and the majority of Research Leaders (RL), to receive training in the TRA process and procedures required.

There are in the order of 80 S&T advisers who will be expected to address TRA issues for major Defence projects. A course should thus be established as soon as possible for the S&T Advisers that covers all elements identified in Table 3. For Chiefs and Research Leaders briefing sessions would probably be sufficient. These sessions should cover at least the DSTO context and TRL/TRA Process elements.

6.2 Pathways

The current 'Pathways' is a flexible program of training, development and support activities designed to accelerate learning and develop knowledge that staff need for a successful career in DSTO and to promote a challenging, supportive learning environment with enhanced job satisfaction. 'Pathways' is designed for 'rookie' DSTO staff providing structured training and development for the first five years of their career in DSTO. Although rookies are unlikely to be intimately involved in undertaking or certifying TRA, an introduction to the practice of TRA, and the reasons for it, could be included in Pathways to establish TRA work as part of DSTO corporate culture.

6.3 Continuing Education Initiative (CEI)

Currently RMIT offers the course 'Risk and Technology Decisions' under the DSTO CEI program. The course is an elective and is delivered on-line to students. Current and new CEI students could be encouraged to take this course.

As a longer-term initiative one of the CEI providers could be asked to develop a course on technical risk assessment for CEI students.

6.4 GPSL and RESMAN

The primary load in conducting and certifying TRA will, in general, fall on DSTO staff at Levels 6 to 8 in the organisation, largely because of the experience required to conduct these activities. GPSL would appear to offer a good opportunity to provide training, and perhaps an opportunity to conduct case studies and assessments for selected projects so that familiarity with the required processes is generated at these key levels in the organisation. If DSTO chooses to introduce risk assessment and management to Tasks, then task-based risk training could also be delivered as part of RESMAN.

6.5 Elements of TRA Training Courses

Table 3 lists the target groups identified for TRA training. TRA training can be thought of as comprising four broad elements:

1. **DSTO Context**. This includes description of the role of DSTO within the Capability Development Process, expected activities and the responsibility for certifying Technical Risk Assessments at first and second-pass approval and support to Projects in developing TRA. The relationships with CDG and DMO, the roles and responsibilities of these agencies and the workings of the 2-pass approval process are also important for understanding the context within which TRA are undertaken and certified.
2. **Risk**. This element covers the current standards for and approaches to Risk Management. It includes scope, definition of terms, the generalised risk

management process, identifying risks, determining the likelihood of them arising and the consequences that could flow from them, and guidelines for establishing and conducting effective risk management.

3. **TRL/TRA Process**. This part of a TRA course would cover the TRL scale, its use for evaluating technology readiness, consideration of systems configuration, integration and implementation issues and the overall approach to TRA within the construct of the Australian 2-pass approval process for Capability Development.
4. **Risk Mitigation**. This element includes the approach to reduction or management of risks in general, the mitigation of risks arising from the introduction of new technology and the identification of appropriate strategies for reducing technical risks in Projects. It could also include material on how technical risks affect cost overruns and schedule slippages.

Table 3: Requirements for TRA Training.

Target Group	Elements of a TRA Course				Delivery
	DSTO context	*Risk*	*TRL/TRA process*	*Risk mitigation*	
S&T Advisers	✓	✓	✓	✓	Tailored course
Task Managers	✓	✓	✓		Elements as part of TM course.
Chiefs/RLs	✓		✓		Briefings
Junior staff	✓	✓			Pathways
CDG IPT members		Invite		Invite	Invite CDG people to DSTO course.
DMO	Input		Input		Input to DMO courses

The last column in the table suggests the way in which the identified training could be provided.

6.6 Priorities for Training

Training for the S&T advisers is seen as critical and it is recommended that this be the first training to be addressed. Because of the oversight role of Chiefs and RL in the certification of TRA, briefing sessions for them are also of prime importance.

As TRA is to become an important part of DSTO S&T activities an introduction to it may be useful for staff in their formative years in the organisation. An appropriately tailored course could form an element of the Pathways program for all new staff. While it is felt that CEI is not an appropriate vehicle for specific TRA training, students could be encouraged to include the current 'Risk and Technology Decisions' course offered on-line by RMIT or a similar course could be requested from the University of South Australia.

The introduction of some elements of TRA training into GPSL and RESMAN courses could also be considered. It may, however, be more effective to introduce such elements into the Task Manager training course as it is likely new Task Managers will also be exposed to TRA work as part of their task and task management activities.

CDG staff on Integrated Project Teams (IPT) may wish to understand the DSTO approach to TRA. Some places could be reserved on the appropriate elements of TRA courses to invite interested CDG staff. The DMO runs an extensive training and staff development program including courses on 'risk'. They may, however, wish to include some elements on TRA into which DSTO could provide input.

7. Resources

Determining the overall impact of TRA work on current DSTO resources is problematic. The undertaking of effective, professional TRA depends upon:

- Maintaining appropriate domain knowledge, technical expertise and relevant experience within DSTO.[8]
- Organising and managing DSTO resources for TRA work.[9]
- Establishing and maintaining useful links with Industry, Academia and other Defence organisations.
- Developing effective working relationships with CDG and DMO.

From the perspective of individual DSTO staff the conduct of TRA requires not only knowledge of the process and procedures described in this paper, but also requires sufficient knowledge of the Project to be able to properly identify the critical technical issues involved and their impact on other aspects of the Project such as cost and schedule. To understand the relevant technologies and their implementation so that technology readiness, system development, integration and demonstration can all be assessed with confidence, may then require significant investment of time and staff resource, up to, and including, the placing of relatively senior staff in major projects.

Additionally, the training of staff in the process, procedures and practice of TRA will impinge upon the time of the staff involved and require specific funding or the re-assignment of other DSTO resources. The ongoing resource implications for DSTO will then depend upon the frequency with which S&T advisers to Projects are changed, staff recruitment, progression and attrition and any changes to the amount of TRA work to be undertaken for Projects. (This depends upon the nature of the Projects, the acquisition approaches used and the levels of technology involved.[10])

It is hoped that the Forward Analysis Plan (FAP) will provide a structured plan for DSTO support to Defence Projects. This could then provide a basis for estimating the impact of TRA work on DSTO resources.

---

[8] As a guide, scientists working in a particular speciality typically spend 2 to 3 hours per week reading the latest published work in their field to maintain their currency. In addition they may attend one or two conferences (including symposia and workshops) per year.

[9] The Policy Tiger Team of the DSTO DPR Implementation and Consultation Team has estimated that, from a 'cold start', TRA Certification could take 12 staff weeks of effort.

[10] For example an overall shift in Defence Projects to more technologically advanced systems could increase the demand on DSTO resources for TRA work.

8. Conclusions

While TRL are useful for evaluating technology readiness, and hence the maturity and feasibility of technologies, they alone do not take account of all systems configuration, integration and implementation aspects. To better understand the technical risks in Defence Projects requires consideration of the use of technology in military operations, broader systems issues such as integration and interoperability with other systems and, ultimately, how the technical aspects of a Project may affect the cost and schedule for acquisition and the capability delivered into service.

To undertake consistent, comprehensive and credible Technical Risk Assessments (TRA) a structured approach is suggested where the TRL scale is used specifically for evaluating technology readiness. This principles-based approach has been designed to fit in with the Australian Capability Development Process, in particular the 2-pass approval process, and it assesses technical risks in accordance with the current Australian Standard (i.e. risks are assessed in terms of consequences and likelihood). To guide the consideration of wider technical risks a series of questions have been developed to encourage structured thinking.

Training requirements for undertaking TRA work are determined and, for the target groups identified, suitable means for delivering this training are suggested. A full course outline was developed and is included in an appendix. Resource implications for DSTO are discussed but the likely costs or impost on current resources could not be adequately estimated owing to significant uncertainties as to how the new TRA work will impinge on DSTO.

9. Acknowledgements

The TRA Tiger Team would like to acknowledge the considerable discussion of the issues surrounding Technical Risk Assessment both within DSTO and the wider ADO community. To all those who have contributed to this discussion: 'thanks'. In particular the team would like to acknowledge the contributions of Joanne Nicholson and Jimmy Ennett who have managed to apply the emerging process and procedures suggested to what can be best described as a 'moving feast'. Their efforts in establishing and refining the TRA pro forma are noted.

10. References

Brock, J. 2004, Best Practices: Using a knowledge-based approach to improve weapon acquisition, *GAO-04-386SP*, US General Accounting Office, January.

Defense Acquisition University 2004, TRL Calculator,
URL: http://acc.dau.mil/simplify/ev_en.php?ID=8796_201&ID2=DO_TOPIC

Graettinger, C.P., Garcia, S., Siviy, J., Schenk, R. J. and Syckle, P.J. 2002, '*Using the Technology Readiness Levels Scale to Support Technology Management in the DoD's ATD/STO Environments*' Special Report CMU/SEI-2002-SR-027.

Graettinger, C. P., & Garcia, S. 2003, 'TRL Corollaries for Practice-Based Technologies' *Proceedings of the Acquisition of Software Intensive Systems Conference, January 29, 2003.*

Kinnaird, Malcolm 2003, *Defence Procurement Review*, 15 August.

Martin, Colin and Smith, Jim 2004, 'Discussion Paper on Implications of Kinnaird Report on DSTO S&T Program Planning', DSTO Internal Paper.

Moon, T., Smith, J., Nicholson, J, Fewell, S. & Duus, A. 2004, 'Technical Risk Assessment: Principles, Process and Procedures', *General Document DSTO-GD-0405*, August.

Roussad, P., Saad, K. and Erickson 1991, *Third Generation R & D* Harvard Business School Press, Boston, Massachusetts.

Standards Australia 2004, *Risk Management AS/NZS 4360:2004*, Joint Standards Australia/ Standards New Zealand Committee, 31 August.

Sud, Ved 2001, 'Research and Development Maturity Assessment Guide with examples from Traffic Flow Management Mire Corporation',
URL: http://www.faa.gov/aua/aua700/organization/mitredoc.pdf

UK MoD 2002, URL: www.ams.mod.uk/ams/content/docs/trlguide.doc

US DoD 2004a, URL: http://www.acq.osd.mil/actd/FY04/TRL%2050002R.doc

US DoD 2004b, *Guide for DoD Acquisition,*
URL: http://www.dau.mil/pubs/gdbks/RMG%20June%2003.pdf

Appendix A: Technology Readiness Levels

Technology Readiness Levels (TRL): descriptions for hardware (HW), Software (SW) and practice-based technologies (PBT). Practice-based technologies include: practices, processes, methods, approaches, schema, frameworks and models.

Technology Readiness Level	Description
1. Basic principles observed and reported	**HW:** Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties. **SW:** Lowest level of software readiness. Basic research begins to be translated into applied research and development. Examples might include a concept that can be implemented in software or analytic studies of an algorithm's basic properties. **PBT:** Scientific, behavioural and market research paper studies.
2. Technology concept and/or application formulated	**HW/SW**: Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies. **PBT:** Practical, speculative applications invented. Potential user communities identified.
3. Analytical and experimental critical function and/or characteristic proof of concept	**HW**: Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative. **SW:** Active research and development is initiated. This includes analytical studies to produce code that validates analytical predictions of separate software elements of the technology. Examples include software components that are not yet integrated or representative but satisfy an operational need. Algorithms run on a surrogate processor in a laboratory environment. **PBT:** Active R&D initiated. Critical elements identified and demonstrated with innovative users.

Technology Readiness Level	Description
4. Component and/or breadboard validation in laboratory environment	**HW**: Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of ad hoc hardware in the laboratory. **SW**: Basic software components are integrated to establish that they will work together. They are relatively primitive with regard to efficiency and reliability compared to the eventual system. System software architecture development initiated to include interoperability, reliability, maintainability, extensibility, scalability, and security issues. Software integrated with simulated current/legacy elements as appropriate. **PBT:** Basic elements integrated to form core PBT. Initial design prototyped and tested.
5. Component and/or breadboard validation in relevant environment	**HW**: Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components. **SW**: Reliability of software ensemble increases significantly. The basic software components are integrated with reasonably realistic supporting elements so that it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of software components. System software architecture established. Algorithms run on a processor(s) with characteristics expected in the operational environment. Software releases are "Alpha" versions and configuration control is initiated. Verification, Validation, and Accreditation (VV&A) initiated. **PBT:** Prototype 'implementation mechanisms' (IM) demonstrated along with core PBT for users in simulated environments (e.g. workshops).
6. System/subsystem model or prototype demonstration in a relevant environment.	**HW**: Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment. **SW**: Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in software-demonstrated readiness. Examples include testing a prototype in a live/virtual experiment or in a simulated operational environment. Algorithms run on processor of the operational environment are integrated with actual external entities. Software releases are "Beta" versions and configuration controlled. Software support structure is in development. VV&A is in process. **PBT:** Implementation mechanisms (IM) refined and integrated with core PBT and demonstrated in relevant environments.

Technology Readiness Level	Description
7. System prototype demonstration in an operational environment.	**HW**: Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft. **SW**: Represents a major step up from TRL 6, requiring the demonstration of an actual system prototype in an operational environment, such as in a command post or air/ground vehicle. Algorithms run on processor of the operational environment are integrated with actual external entities. Software support structure is in place. Software releases are in distinct versions. Frequency and severity of software deficiency reports do not significantly degrade functionality or performance. VV&A completed. **PBT:** Implementation needs of mainstream users identified and integrated into prototype. Operational use by relevant users demonstrated across the community.
8. Actual system completed and qualified through test and demonstration.	**HW**: Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications. **SW**: Software has been demonstrated to work in its final form and under expected conditions. In most cases, this TRL represents the end of system development. Examples include test and evaluation of the software in its intended system to determine if it meets design specifications. Software releases are production versions and configuration controlled, in a secure environment. Software deficiencies are rapidly resolved through support infrastructure. **PBT:** Technology adopted and distributed for widespread use across the community of practice.
9. Actual system proven through successful mission operations.	**HW**: Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation (OT&E). Examples include using the system under operational mission conditions. **SW**: Actual application of Software in its final form and under mission conditions, such as those encountered in OT&E. In almost all cases, this is the end of the 'debugging' phase of system development. Examples include using the system under operational mission conditions. Software releases are production versions and configuration controlled. Frequency and severity of Software deficiencies are at a minimum. **PBT:** Technology is used routinely within community of practice. Best practices, quality assurance and body of knowledge are in place.

Appendix B: System Readiness Levels (SRL)

System Readiness Levels (SRL) refer to total, integrated systems. When assessing the operational readiness of a system, a system of systems or a family of systems, all systems aspects should be taken into account. In addition to the integration of hardware, software (and any practice-based technologies), these include taking account of organisational structure, policies, processes and practices, operational concepts, doctrine and tactics, facilities, logistics and support, staffing, training and workforce planning.

B.1. Short version

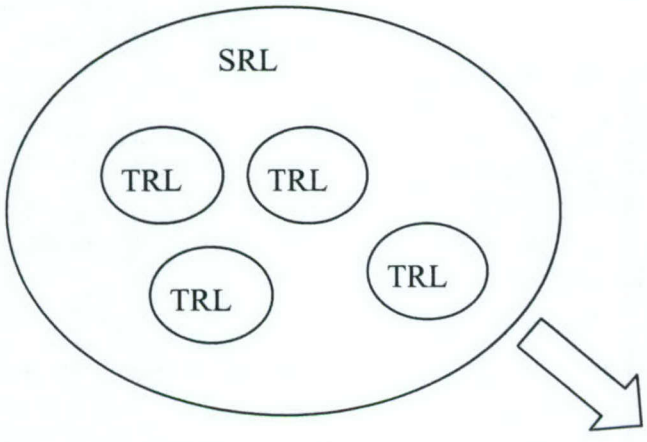
SRL 1: Basic principles observed and reported.
SRL 2: System concept and/or application formulated.
SRL 3: Analytical studies and experimentation on system elements.
SRL 4: Sub-system components integrated in a laboratory environment.
SRL 5: System tested in a simulated environment.
SRL 6: System demonstrated in a simulated operational environment, including interaction with simulations of external systems.
SRL 7: Demonstration of system prototype in an operational environment, including interaction with external systems.
SRL 8: System proven to work in the operational environment, including integration with external systems.
SRL 9: Application of the system under operational mission conditions.

B.2. Longer version

System Readiness Level	Description
1. Basic principles observed and reported	Lowest level of system readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a system's basic properties.
2. System concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the system. Examples might include COTS components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment	Basic system components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.

5. Component and/or breadboard validation in relevant environment	Fidelity of system components increases significantly. The basic system components are integrated with reasonably realistic supporting elements so the total system can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components into system elements.
6. System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is demonstrated in a well-simulated operational environment, including interaction with simulations of key external systems.
7. System prototype demonstration in an operational environment	Prototype near, or at, planned operational system. Represents a major step up from SRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space, including interaction with external systems.
8. Actual system completed and qualified through test and demonstration	System has been proven to work in its final form and under expected conditions, including integration with external systems. In almost all cases, this SRL represents the end of true system development. Examples include test and evaluation of the system in its intended context and operational architecture to determine if it meets design specifications.
9. Actual system proven through successful mission operations	Actual application of the system in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Appendix C: TRL, SRL and TRA Relationship



TRA

Event	Likelihood	Impact(s)	Mitigation Measures
1			
2			
3			
.			
.			
.			
n			

In addition to immature technologies, the application of mature technologies to the particular system in question may result in technical risks occurring. Not only is there the potential for technical risks to arise in the internal integration of systems employing mature technologies (which should be highlighted by the SRL process), there is also the possibility that mature technologies may not be well applied to the problem at hand.

An example is the perennial issue of weight growth in combat aircraft – in general this may occur because loads have been under estimated (aerodynamics); structures have been inadequately designed (materials and structural design techniques); material properties differ from those assumed (materials TRL could point to this); inadequate attention has been paid to equipment space and cooling requirements (SRL might highlight this); or failure to prevent requirements creep (program management issue).

TRL and SRL assessments should be viewed as inputs to the TRA, which then focuses on the particular risk events identified, their probability, the consequences arising from them, their impact on the Project and possible mitigation measures. TRL and SRL assessments can thus inform the TRA, but are not a substitute for it.

Appendix D: Guidelines for Assessing Technical Risk

Determining Technology Readiness Levels

1. First step: Identify key technologies.
2. Work 'from the outside in'.
3. Identify the system boundaries.
4. Identify the key subsystems.
5. Identify the technologies that must be delivered if the expected subsystem capabilities are to be achieved.
6. Assess the degree to which these technologies have been demonstrated, and then evaluate the TRL.

N.B. Internal and external integration issues will be addressed in TRA.

Completing a Technical Risk Assessment

1. First step: Define the Parameters used to describe the risks, the ranges used to define Likelihood, and the descriptors used to assess Impact (Consequences).[11]
2. Apply structured thinking to draw out potential issues with the system, subsystems, components and the integration of these. Typically, at 2nd pass the impact statements will be more detailed than at 1st pass.
3. Categorise the relevant technical risks through a comparative assessment of their likelihood and impact. This information is usually presented as a 'risk table'.
4. Identify possible risk mitigation strategies.

When assessing technical risk the following questions provide a guide for structured thinking:

- **Is the proposal technically sound?** (Provide an assessment of underlying technical, or technically driven program aspects.)
- **Is it likely to work as required by the prime Customer?** (Assess the way in which technical issues, including integration, are being addressed in the system originator's program.)
- **Will the proposal meet Australian capability requirements?** (The critical issue here is what it means for Australia as a potential Customer.)
- **To what degree, and how, will the risks adversely affect, or be affected by, other projects planned or currently in progress across the ADF?** (Consider external integration and constraints.)

[11] In general, these will be highly context dependent. For example, the measures of likelihood for risks in safety assessments are likely to be much smaller than those in project assessments.

Appendix E: TRA Course Outline

Context

Approvals process
Committee Structure
Standing Briefs
Implementation of the Defence Procurement Review - DSTO roles/ remit

- TRL
- Technical risk

Risk Policy

- Project ownership & responsibility for risk assessment and management
- DSTO role in certification of risk assessments
    - Project assessments
    - DSTO technical risk assessments
    - Third-party risk assessments

Why does Defence need to understand and manage risk?

What are TRL?

- Background
- Principle - evidence-based assessment of technology maturity
- Emphasis on demonstrated application
- Nine-level Definition Table

How might TRL be used?

A filter for identifying technology development needs

What is Technical Risk?

Principles-based approach.
Definition of Risk:

- Risk management standard AS/NZ 4360:2004
- Likelihood & Impact
- Different impacts, linked to program context

Examples:

- From ordinary life
- From projects
- From safety assessments

Stressing the importance of context.
Noting the difference between TRA and TRL.

What are SRL?

How might these be used?
Identifying systems configuration, integration (internal and external) and implementation issues.

Risk tabulations

- Importance of definition of terms used for likelihood and impact.
- 3 x 3 tabulation
- Contrast to 5 x 5 tabulation
- Examples

Risk aggregation and analysis

Assessment of risk tabulations
Analysis tools

- Risk independence
- Relationship to programme plan

Certification of Technical Risk Assessments (How to do this?)

Understand the project:

- What are the options?
- What technologies are critical to delivery of capability for each?
- How mature are they?

Understand the context:

- What dependencies exist?
- What internal integration issues exist?
- What external integration issues exist?

Are all these issues captured in the risk assessment?
Are the likelihood and impact estimates credible?
Are the risk mitigation measures reasonable?

Structured questions:

- Is the programme technically sound?
- Will the system deliver the capability expected by the primary Customer?
- Will it deliver the required capability for Australia in the Australian operating environment?
- Can we be confident about those costs that may be considered 'technically-driven'?

For second pass assessment:

- Compare 2nd pass assessment with 1st pass.
- Assess whether changes in the risk assessment are credible and driven by identifiable management or Contractor action.
- Identify any further risk mitigation measures to be taken post 2nd pass (e.g. location of DSTO SME in Contractor teams; T&E; acceptance criteria etc).
- Do the Contractual arrangements reflect measures to mitigate identified technical risks?
- Re-assessment of TRL & SRL.
- Review of dependencies and impacts on other projects.
- Greater detail, particularly of probable impacts.
- Linkage to delivery of the required (and Contracted) capability.

DISTRIBUTION LIST

Technical Risk Assessment of Australian Defence Projects

DSTO Tiger Team for Technical Risk Assessment: Jim Smith (Chairman), Graeme Egglestone, Paul Farr, Terry Moon, David Saunders, Peter Shoubridge, Kym Thalassoudis and Tony Wallace

AUSTRALIA

DEFENCE ORGANISATION

	No. of copies
S&T Program	
Chief Defence Scientist	shared copy
FAS Science Policy	
AS Science Corporate Management	
Director General Science Policy Development	
Counsellor Defence Science, London	Doc Data Sheet
Counsellor Defence Science, Washington	Doc Data Sheet
Scientific Adviser to MRDC, Thailand	Doc Data Sheet
Scientific Adviser Joint	1
Navy Scientific Adviser	1
Scientific Adviser - Army	1
Air Force Scientific Adviser	1
Scientific Adviser to the DMO M&A	1
Scientific Adviser to the DMO ELL	1
Platforms Sciences Laboratory	
Director Platforms Sciences Laboratory	1
Chief of Air Vehicles Division	1
Research Leader Aircraft Materials	1
Research Leader Propulsion Systems	1
Research Leader Aircraft Structures	1
Research Leader Flight Systems	1
Chief of Maritime Platforms Division	1
Research Leader Signature Management	1
Research Leader Structures, Mechanical and Electrical	1
Research Leader Surface Platform Systems	1
Research Leader Undersea Platform Systems	1
Head CBRN	1
Head Strategic Policy & Plans	1
Graeme Egglestone	1
Systems Sciences Laboratory	
Director Systems Sciences Laboratory	1
Chief of Air Operations Division	1
Research Leader Air Operations Analysis	1
Research Leader Crew Environments & Training	1
Research Leader Airborne Mission Systems	1
Chief of EWR Division	1

Research Leader RF Electronic Warfare	1
Research Leader Electronic Warfare Systems	1
Research Leader Electro-Optic Electronic Warfare	1
Research Leader Microwave Radar	1
Chief of Land Operations Division	1
Research Leader Land Capability Studies	1
Research Leader Land Systems	1
Research Leader Human Systems Integration	1
Chief of Maritime Operations Division	1
Research Leader Maritime Sensor Systems	1
Research Leader Maritime Combat Systems	1
Research Leader Littoral Warfare	1
Research Leader Maritime Operations Research	1
Paul Farr	1
Chief of Weapons Systems Division	1
Research Leader Air Weapons Systems	1
Research Leader Emerging Weapon Technology	1
Research Leader Land Weapons Systems	1
Research Leader Maritime Weapons Systems	1
Dr Kym Thalassoudis	1
Information Sciences Laboratory	
Director Information Sciences Laboratory	1
Chief of C2D Division	1
Research Leader Command & Intelligence Environments	1
Research Leader Military Information Enterprise	1
Research Leader Theatre Command Analysis	1
Chief of Defence Systems Analysis Division	1
Research Leader Integrated Capabilities	1
Research Leader Planning and Guidance	1
Research Leader Strategy and Concepts	1
Head Capability Planning & Prioritisation	1
Head Studies Guidance	1
Dr Jimmy Ennett	1
Chief of Information Networks Division	1
Research Leader Information Assurance	1
Research Leader Military Communications	1
Chief of ISR Division	1
Research Leader Imagery Systems	1
Research Leader Secure Communications	1
Research Leader Wide Area Surveillance	1
DSTO Library and Archives	
Library Edinburgh	2
Defence Archives	1
Capability Development Group	
Director General Maritime Development	1
Director General Land Development	1
Director General Aerospace Development	1
Director General Capability and Plans	1

Assistant Secretary Investment Analysis 1
Director Capability Plans and Programming 1
Director Trials 1

Chief Information Officer Group

Deputy CIO Doc Data Sheet
Director General Information Policy and Plans Doc Data Sheet
AS Information Strategy and Futures Doc Data Sheet
AS Information Architecture and Management Doc Data Sheet
Director General Australian Defence Simulation Office Doc Data Sheet
Director General Information Services Doc Data Sheet

Strategy Group

Director General Military Strategy Doc Data Sheet
Director General Preparedness Doc Data Sheet
Assistant Secretary Strategic Policy Doc Data Sheet
Assistant Secretary Governance and Counter-Proliferation Doc Data Sheet

Navy

SO (SCIENCE), COMAUSNAVSURFGRP, NSW Doc Data Sht & Dist List
Maritime Operational Analysis Centre, Building 89/90 Garden Island Sydney
Deputy Director (Operations) }
Deputy Director (Analysis) } Doc Data Sht & Dist List
Director General Navy Capability, Performance and Plans, Navy Headquarters Doc Data Sheet
Director General Navy Strategic Policy and Futures, Navy Headquarters
Doc Data Sheet

Air Force

SO (Science) - Headquarters Air Combat Group, RAAF Base, Williamtown NSW 2314 Doc Data Sht & Exec Summ

Army

ABCA National Standardisation Officer, Land Warfare Development Sector, Puckapunyal e-mailed Doc Data Sheet
SO (Science) - Land Headquarters (LHQ), Victoria Barracks NSW
Doc Data & Exec Summ
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera QLD
Doc Data Sheet

Joint Operations Command

Director General Joint Operations Doc Data Sheet
Chief of Staff Headquarters Joint Operations Command Doc Data Sheet
Commandant ADF Warfare Centre Doc Data Sheet
Director General Strategic Logistics Doc Data Sheet

Intelligence and Security Group

DGSTA Defence Intelligence Organisation 1
Manager, Information Centre, Defence Intelligence Organisation 1 (PDF)
Assistant Secretary Capability Provisioning Doc Data Sheet

Assistant Secretary Capability and Systems — Doc Data Sheet
Assistant Secretary Corporate, Defence Imagery and Geospatial Organisation — Doc Data Sheet

Defence Materiel Organisation

Deputy CEO — 1
Head Aerospace Systems Division — 1
Head Maritime Systems Division — 1
Chief Joint Logistics Command — 1
Head Materiel Finance — 1

Inspector General

Director Enterprise Risk Management — 1

Defence Libraries

Library Manager, DLS-Canberra — 1
Library Manager, DLS - Sydney West — Doc Data Sheet

OTHER ORGANISATIONS

National Library of Australia — 1
NASA (Canberra) — 1

UNIVERSITIES AND COLLEGES

Australian Defence Force Academy
- Library — 1
- Head of Aerospace and Mechanical Engineering — 1

Serials Section (M list), Deakin University Library, Geelong, VIC — 1
Hargrave Library, Monash University — Doc Data Sheet
Librarian, Flinders University — 1

OUTSIDE AUSTRALIA

INTERNATIONAL DEFENCE INFORMATION CENTRES

US Defense Technical Information Center — 2
UK Dstl Knowledge Services — 2
Canada Defence Research Directorate R&D Knowledge & Information Management (DRDKIM) — 1
NZ Defence Information Centre — 1

ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service — 1
Engineering Societies Library, US — 1
Materials Information, Cambridge Scientific Abstracts, US — 1
Documents Librarian, The Center for Research Libraries, US — 1

SPARES — 5

Total number of copies: Printed 101 PDF 1 = 102

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Technical Risk Assessment of Australian Defence Projects

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

DSTO Tiger Team for Technical Risk Assessment:

Jim Smith (Chairman), Graeme Egglestone, Paul Farr, Terry Moon David Saunders, Peter Shoubridge, Kym Thalassoudis and Tony Wallace

5. CORPORATE AUTHOR

Information Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-1656	AR-013-285	Technical Report	December 2004

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2004/1050591	STR 04/254	CDS	25	13

13. URL on the World Wide Web

http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-1656.pdf

14. RELEASE AUTHORITY

Chief, Defence Systems Analysis Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

Risk assessment, Risk management, Defence procurement, Defence technology

19. ABSTRACT

The Defence Procurement Review (DPR) recommended sweeping changes to Defence Department structures, policies, processes and procedures for the acquisition of military capabilities. As a result of the Government's acceptance of the recommendations of the DPR, DSTO roles and responsibilities now include guidance on, and certification of, Technical Risk Assessments (TRA) for major acquisition proposals up to second-pass approval. This paper provides a structured approach for the undertaking of TRA and their subsequent certification. Also included are discussions of the underpinning principles, techniques and tools, training requirements and resource implications.